

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

DOCKET FILE COPY ORIGINAL

RECEIVED

DEC 17 2002

FEDERAL COMMUNICATIONS COMMISSION
OFFICE OF THE SECRETARY

In the Matter of)

Implementation of the)

Telecommunications Act of 1996:)

CC Docket No. 96-115

Telecommunications Carriers' Use of)

Customer Proprietary Network Information)

And Other Customer Information)

REPLY COMMENTS OF THE
U.S. DEPARTMENT OF JUSTICE AND
THE FEDERAL BUREAU OF INVESTIGATION

The U.S. Department of Justice ("DOJ") and the Federal Bureau of Investigation ("FBI"), pursuant to Federal Communications Commission ("FCC" or "Commission") Rules 1.415 and 1.419,¹ submit the following Reply Comment in response to the Commission's Third Further Notice of Proposed Rulemaking (Third Further Notice) in the above-docketed proceeding.

SUMMARY

In its Notice, the Commission seeks to refresh the record, *inter alia*,² with respect to issues involving the regulation of foreign storage of and access to domestic Customer Proprietary Network Information ("CPNI"). The DOJ and FBI ask the Commission to hold that the CPNI of U.S. customers who subscribe to domestic telecommunications services, as described at greater length in Section II, be stored exclusively within the United States. Similarly, the DOJ and FBI ask that the Commission constrain foreign access to such information, under the circumstances

¹ 47 C.F.R. §§ 1.415 and 1.419

² The Commission also seeks comment in the instant docket as to any need for additional enforcement mechanisms or protections for carrier proprietary information and the implications of the Commission's CPNI regulations when carriers leave the market. Our comment applies solely to the issues of foreign storage and access.

described below in Section II. Such rulings will secure inextricably-related and important U.S. equity interests: the maintenance of U.S. national security and public safety, the preservation of effective law enforcement and the efficacy of U.S. legal process, the protection of the privacy and confidentiality of communications records of U.S. customers who subscribe to domestic communications, and the prevention of espionage, including economic espionage. In taking this position, the DOJ and the FBI also recognize, as discussed in Section II, that there are logical contextual exceptions to the general rule we propose. Such exceptions would permit foreign storage of and access to such information under circumstances that are limited in nature, scope, and duration, and which offer balance in a global communications environment.

Section I: Background

On May 22, 1997, a security agreement³ was consummated between British Telecommunications plc (“BT”) and MCI Communications Corporation (“MCI”), on the one hand, and the U.S. Department of Defense (“DOD”) and the FBI, on the other, arising out of a merger between BT and MCI with respect to the creation of Concert plc, a transaction then before the Commission.⁴ In granting approval to the transaction, the Commission made the authorizations and licenses related to the transaction subject to, and conditioned the authorizations and licenses upon, compliance with the provisions of the agreement.⁵ In the BT-MCI agreement, the matter of CPNI storage and access arose, with its treatment in Section D.1-3 as follows:

³ The FBI and DOJ have negotiated a number of such agreements in the context of foreign ownership and the foreign location of telecommunications facilities that support the provisioning of telecommunications service in the United States. These agreements have included provisions aimed at ensuring that the government in the U.S. can satisfy its obligations to preserve the national security and enforce the laws, and protect the public safety, as well as ensure the security of communications and related records and information in order to protect the privacy of Americans and to prevent espionage, including economic espionage.

⁴ See *In the Matter of the Merger of MCI Communications Corporation and British Telecommunications plc (BT-MCI Merger)*, GN Docket No. 96-245.

⁵ *Id.* Commission's grant of authority issued August 21, 1997

1. For purposes of this subsection and related provisions of the Implementation Plan, "Domestic Customer" means a customer who subscribes to Domestic Telecommunications Services provided by Affiliates and whose international service is not provided pursuant to a contract or tariff arrangement for international services or similar volume discount arrangement. Use of a telephone calling card or similar device outside the United States does not change a customer's status as a Domestic Customer.

2. Except for CPNI generated as a result of international calls, it is MCI's general practice to store and maintain all CPNI for Domestic Customers within the United States. Affiliates have no intention of materially increasing in the near future the degree of access from outside the United States to CPNI pertaining to Domestic Customers.

3. The FCC presently has pending before it a rulemaking proceeding concerning CPNI (Common Carrier Docket 96-115). The FBI and MCI may submit to the FCC in this Docket comments regarding the issue of access to and storage of CPNI outside the United States. Until the earlier of March 31, 1998, or the effective date of the FCC regulations specifically related to this issue, CPNI pertaining to Affiliates' Domestic Telecommunications Services (i) shall be stored and maintained exclusively in the United States, and (ii) shall not be accessible from outside the United States to a materially greater degree than at present. The preceding sentence shall not apply to any Domestic Customer who has approved having his or her CPNI accessible from outside the United States. After the earlier of March 31, 1998, or the effective date of any FCC regulations specifically related to this issue, Affiliates (i) shall comply with those regulations, and (ii) shall in any event, store and have accessible in the United States a copy of all CPNI retained by MCI in the ordinary course of business pertaining to telecommunications that originate or terminate in the United States. The Parties' agreement on provisions relating to CPNI in this Agreement ... shall be without prejudice to the positions they may choose to take in any proceeding with respect to this issue.⁶

As can be seen, in reviewing Section D.1, a "Domestic Customer" in the BT-MCI agreement meant a customer who subscribed to Domestic Telecommunications Services' provided by the Affiliates (i.e., BT, MCI, and Concert, and each of them individually) *and* whose international service is "not provided pursuant to a contract or tariff arrangement for international services or similar volume discount arrangement." Thus, a Domestic Customer's

⁶ *BT-MCI Merger Agreement*, CY Docket No. 96-245, at 7.

"Domestic Telecommunications Services" are defined in the BT-MCI agreement as meaning "the provision of telecommunications services from one U.S. location (any state, district, territory, or possession of the United States) to another U.S. location." *BT-MCI Agreement* at 2.

“service” comprehended both intra-United States communications as well as non-volume-discounted international communications. Put differently, Domestic Customers would have constituted the vast majority of MCI's subscribers (i.e., subscribers who did *not* have substantial international calling patterns or usage). The DOD and the FBI sought to assure the security of U.S. telecommunications and related records and information *in order to protect the privacy of Americans* by preventing access to those records in foreign countries.⁸ Accordingly, it seemed highly appropriate to the DOD and FBI to insist upon provisions to protect the privacy of subscribers who never, or only relatively rarely, place international calls, by not having their communications records and information (CPNI) stored or accessed abroad, with all intra-U.S.-based CPNI being required to be maintained exclusively within the United States.⁹ The fundamental reason for pressing for such a provision was the DOD and FBI's considered assessment that, once a subscriber's CPNI was stored or readily acquirable outside the United

⁸ The DOJ and the FBI share the views expressed by numerous other commenters who forcefully argue that privacy protection of a subscriber's telecommunications records and information, including CPNI, is absolutely vital. *See* the Commission's description of the highly personal nature of CPNI at 9-10, *infra*. Although privacy protection is sometimes cast in terms of protecting an individual's private matters from the prying eyes of government, within the United States there are numerous privacy-protecting regimes that ensure that U.S. governmental access to private material is appropriately balanced, based upon Constitutional and privacy-protecting statutory dictates, and is tied to legal process, including warrants and court orders, appropriate to the level of the privacy interest involved. However, placing private CPNI records overseas effectively diminishes the privacy protection embodied in U.S. law, effectively prevents detection of privacy (CPNI) abuse, and precludes meaningful privacy (CPNI) protection oversight and control by entities such as the FCC, executive branch agencies, the U.S. courts, Congress, and other representatives elected by the subscribers.

⁹ From a compliance perspective, there is a conceptually similar *protective* provision in the *BT-MCI Agreement*.

Affiliate facilities referred to in the preceding paragraph will be capable of complying, and configured to comply, and Affiliates' officials in the United States will have unconstrained authority to comply with [various National Security Emergency Preparedness and other U.S. laws] (emphasis added). *BT-MCI Agreement* at 5, Section II, B.

This provision was intended to ensure that no foreign law or authority would or could impinge upon the full and unequivocal effect of U.S. law. In other words, U.S. law would exclusively control. Contrast these provisions with the issue of foreign storage of, or broad access to, the CPNI of U.S. Domestic Customers which is now before the Commission in this docket, and which, as pointed out in our Comment, if permitted, would open the door to the operation of foreign law (in potential contravention of U.S. law).

States. U.S. law would no longer be the sole source of controlling law.

Thus, notwithstanding that the Congress has enacted certain privacy and confidentiality-based laws (such as those pertaining to **CPNI**¹⁰ in the Telecommunications Act of 1996 and to other telecommunications customer records and information in the Electronic Communications Privacy Act of 1986)¹¹ with the clear intention of securing U.S. telecommunications customers' privacy, these laws could be circumvented and their purpose frustrated by the storage of U.S. **CPNI** in a foreign country. Indeed, the very **CPNI** statutory provision which aims at securing the privacy and confidentiality of **CPNI**, and which regulates the use, disclosure, and access of **CPNI** by telecommunications carriers," contains the carve-out "[e]xcept as required by law...." Hence, the invocation of foreign law by foreign governmental entities, including foreign intelligence services, could lead either to the narrow tactical acquisition of the **CPNI** of certain U.S. customers (including the proprietary and highly-sensitive **CPNI** of specific **U.S.** corporate customers)" or to the broad-scale strategic acquisition of **CPNI** of a great many customers by such foreign entities.

To take perhaps the most harrowing example, if it were the case that *all* telecommunications carriers were permitted to store *all* of their U.S. subscribers' **CPNI** abroad, consider the implications of exposing the highly-sensitive **CPNI** records of *all* of the U.S. Government departments and agencies – where **CPNI customer profiles** would reveal executive branch, congressional, judicial, military, diplomatic, civil, law enforcement, and intelligence

¹⁰ See 47 U.S.C. §222

¹¹ See Pub. L. 99-508, Title II, as amended, codified at 18 U.S.C. §2703

¹² See 47 U.S.C. 222(c)(1)

¹³ As discussed below, such access to the proprietary and business-sensitive CPNI records and information of U.S. corporations would furnish an obvious entree and method for conducting economic espionage.

communications records, and thereby disclose highly-sensitive U.S. Governmental actions, activities, and contacts.

Moreover, and importantly, foreign acquisition of the CPNI of U.S. customers may never be delectable or reported within the United States if the foreign legal directive or process involved, like typical U.S. process, included a provision directing the carrier (or a contractor of a carrier, as the case may be) *not* to disclose the existence of the fact of the foreign acquisition or anything about the information being acquired

On July 9, 1997, the FBI filed an *ex parte* comment letter with the Commission in the instant docket (hereafter “FBI *ex parte* letter”)“, which identified at length issues associated with the foreign storage of, and access to, the CPNI of U.S. customers who only subscribe to domestic telecommunications services (i.e., Domestic Customers). We incorporate by reference the *ex parte* letter in its entirety here. In the *ex parte* letter, Domestic Customers are described as:

customers, both individuals and businesses, whose telecommunications service (and whose CPNI related to such service) is essentially intra-U.S. in nature. Such service would encompass conventional long distance service, including long distance service where international calls may be placed; but it would be distinguished from international service(s) provided pursuant to special contract or tariff arrangement for international services or similar volume discount arrangement.”

The FBI recommended to the Commission that it “mandate that the CPNI of Domestic Customers ... be exclusively stored in (accessible from) the United States.”“ We noted that “distinct and deleterious national security, law enforcement, public safety, business proprietary, and privacy concerns are raised when foreign-based storage of, or direct foreign access to, the

¹⁴ Letter from John F. Lewis, Jr., Assistant Director, National Security Division, Federal Bureau of Investigation, to William F. Caton, Acting Secretary, Federal Communications Commission (“FBI *ex parte* letter”), CC Docket No. 96-115 (filed July 9, 1997).

¹⁵ *Id.* at 1, n.1.

¹⁶ *Id.* at 1.

CPNI of Domestic Customers is permitted.”¹⁷ Elsewhere in the letter, we pointed out that, although distinct, the array of concerns noted were inextricably interwoven with the matter of the privacy and confidentiality of CPNI.¹⁸

In the FBI *ex parte* letter, we presented a detailed explanation of the harms to law enforcement and public safety,¹⁹ national security and international espionage,” economic espionage and access to proprietary business information,” and subscriber CPNI privacy,” if the CPNI of Domestic Customers could be stored and accessible abroad. For example, we noted in the *ex parte* letter:

The CPNI of governmental officials may well disclose telephone contacts which would suggest to a foreign intelligence officer that the U.S. official could be “recruited,” “blackmailed,” or “compromised.” For example, a U.S. official’s contacts with banks, credit bureaus, etc.; counseling agencies or alcohol or drug counseling entities; sexual liaison contacts; etc. could give a foreign power the intelligence and leverage needed to recruit the U.S. official, leading to espionage and other grave national security harm.²³

Such dangers would not be limited to governmental officials. The Government could not assure U.S.-resident private persons the same degree of privacy if their CPNI is stored outside the U.S. as if it were stored within the U.S. Thus ordinary persons could be exposed to various crimes in which CPNI would be useful, such as fraud, identity theft, extortion, and child abductions in

¹⁷ *Id.*

¹⁸ “[S]ubstantial governmental, business, societal concerns [are] *interrelated* with the concern of customer privacy.” (emphasis added) *Id.* at 3, n.5.

¹⁹ *Id.* at 4.

²⁰ *Id.* at 6.

²¹ *Id.* at 8.

²² *Id.* at 10.

²³ *Id.* at 8, n 18.

custody disputes

Further, in the *ex parte* letter, we asserted that “the preservation of privacy interests, *inter alia*, would be illusory if foreign-based storage of, or direct foreign-based access to, CPNI [of Domestic Customers] is permitted, and that, with foreign access, the FCC’s preemption [in CPNI regulation/enforcement] is, in fact, not certain nor clearly dispositive:”

If foreign storage of, or direct foreign access to, such CPNI is permitted ... the laws and (or) the practices of the foreign country where the CPNI is stored, or from which it can be electronically accessed, could effectively nullify and supersede provisions of U.S. law related to CPNI. Stated differently, although FCC rules and regulations regarding CPNI would be preemptive within the U.S., and control CPNI exclusively, the same cannot be said when the jurisdictional reach and laws of another country are implicated through foreign-based storage or foreign-based direct access. Moreover, the prospect of direct foreign access to the CPNI of U.S. Domestic Customers would have the unintended effect of seriously undermining, legally and practically, important U.S. Governmental, business-proprietary, and privacy-based protections that are afforded to CPNI under international and bilateral treaties (e.g., Mutual Legal Assistance Treaties (MLATS) and other international legal assistance procedures (e.g., Letters Rogatory)).”

We argued that permitting such foreign storage and access “would, as a practical matter [owing to the application of foreign law and/or practice], constitute FCC endorsement of the paradigm that certain customers can properly be accorded disparate, and greatly-reduced privacy protections, thereby creating a two-tiered regime, wherein there is created ‘second-class citizen’-CPNI telecommunications privacy rights.”²⁶ Such storage and access “would undermine reasonable subscriber assumptions about the safety, security, and business-proprietary and privacy protections that normally would be expected to exist under U.S. law.”

We also noted that “foreign storage or direct electronic foreign access should never be

²⁴ *Id.* at 2, n. 2.

²⁵ *Id.* at 3 (footnotes omitted).

²⁶ *Id.* at 9, n. 21.

²⁷ *Id.* at 9.

permitted to occur absent clear, affirmative, and informed written customer consent” (e.g., I, [customer], hereby authorize Carrier X to store my CPNI in [country Y] and/or...direct foreign electronic access to my CPNI from [country Y]).²⁸ Additionally, in the FBI *ex parte* letter, we stated with regard to U.S.-based customers *outside the category of Domestic Customers* that it is imperative that a “copy” of those customers’ CPNI be stored in the United States, owing to the critical need for prompt, secure, and confidential law enforcement, public safety, or national security access to such information pursuant to lawful authority.”

Finally, although the impetus for the recommended action arose from a foreign acquisition case, we noted that the harms associated with foreign storage and access would logically apply without regard to foreign ownership, and thus should apply to *all* telecommunications carriers, domestic or foreign-based, offering service in the United States to Domestic Customers. Hence, treatment of these issues was appropriate for the Commission under the aegis of a rule-making proceeding dealing with CPNI which would have comprehensive effect with respect to all carriers. As noted above, BT, MCI, Concert, the DOD, the FBI, and the Commission (which at the time of the agreement was consulted) agreed that this docket was the proper forum

Section 11. Description of Domestic Customers; Service Usage; Exceptions

In order that the Commission and other commenters in the instant docket can better understand the context and parameters of the recommended actions (and the nature of our concern), we believe it is important to further outline them here. Before proceeding, however, we wish to underscore the extremely sensitive nature of CPNI; we reiterate the Commission’s

²⁸ *Id.* at 9. To be clear, we are contemplating the case where the foreign storage of and/or access to CPNI is sustained and comprehensive in nature, scope, and duration (see our discussion at 11-12, *infra*). We are not suggesting that customer consent should be required when a U.S. customer’s CPNI is briefly disclosed incidental to certain international calling or roaming functions, where *ad hoc* disclosure of a limited amount of a customer’s CPNI is necessarily required for call set-up, authentication, and billing.

²⁹ *Id.* at 4, n. 8

prior description of CPNI:

Much CPNI, however, consists of highly personal information, particularly relating to call destination, including the numbers subscribers call and from which they receive calls, as well as when and how frequently subscribers make their calls. This data can be translated into subscriber profiles containing information about the identities and whereabouts of subscribers' friends and relatives;³⁰ which businesses subscribers patronize; when subscribers are likely to be home and/or awake; product and service preferences; how frequently and cost-effectively subscribers use their telecommunications services; and subscribers' social, medical, business, client, sales, organizational, and political telephone contacts."

In describing U.S. Domestic Customers, we have in mind what we believe are the most typical, and by far the most numerous, of U.S. subscribers. Such subscribers, whether to wireline or wireless service, make local calls" and long distance calls within the United States. Moreover, they make limited international calls. Such calling may be through conventional means or through pre-paid cards or similar devices. As such, this calling information (including its attendant call set-up, billing, and related information and records), practically speaking, has little or no reason to be stored outside the United States.³⁴

³⁰ Since the time of the quoted Commission's language, Section 222 was amended in 1999 so as now to include and provide privacy protection for "call location information." See Pub.L. 106-81, § 5(1)-(4) (1999). Foreign access to, and abuse of, such call location information could be very detrimental to U.S. mobile subscribers.

³¹ *Second Report and Order and Further Notice of Proposed Rulemaking (CPNI Order)* at 48-49, ¶61, CC Docket No. 96-115 (rel. Feb. 26, 1998), 13 FCC Rcd at 8108,761 (emphasis added).

³² While flatrate billing is the norm for wireline services, certain wireline and many wireless services maintain local call detail, thereby exposing frequently made calls to foreign scrutiny should the CPNI be located outside the U.S.

³³ Other electronic communications, messaging, signaling, and similar traffic are nowadays frequently interwoven with conventional telephony services. Such communication, messaging, and signaling information likewise may be maintained by carriers and thus subject to foreign scrutiny if it is stored outside the United States.

³⁴ We contrast the calling of Domestic Customers with the international services and plans that may attract large multinational corporations which conduct substantial business in many different countries and for whom certain special contract and/or tariff arrangements or similar volume discount arrangements may make sense. As to such corporations, they already expose a substantial amount of their international communications abroad; foreign-based (foreign-rendered) services and networks would already capture a significant amount of CPNI-like information; and by doing business in a variety of foreign countries, such corporations have already subjected themselves to the laws of those countries (to include those that permit governmental authorities (or perhaps others) to obtain CPNI-like information resident in that country).

We recognize that with certain international long distance calling, and foreign roaming, CPNI call setup and billing information may need to be transmitted (and briefly stored and accessible) internationally through various carrier networks in order to support the provisioning of the service.³⁵ Such information would exist in a foreign country briefly as part of the call set-up and authentication, and for billing purposes. Although the foreign presence of such CPNI arguably exposes that particular information to the harms we outlined in Section I, the exposure is clearly fleeting and quite limited.

Consequently, in terms of the interrelated concerns noted above, we do not object to the very limited foreign storage of or access to the CPNI of Domestic Customers in the context of setting-up and billing for particular international calls or for international roaming.

Far and away the most problematic in nature, scope, and duration is a carrier's foreign storage of, or broad foreign access to, CPNI.³⁶ This can exist with respect to a carrier offering multinational service or to a purely domestic carrier through a contractual relationship with a foreign-based, third-party billing or marketing contractor, for example. Making such circumstances worse from the perspective of the privacy and confidentiality³⁷ of customer CPNI material is the prospect that the CPNI involved may be that of a carrier's entire customer base. The storage or access thus may well be ongoing and comprehensive, with, for example, monthly

³⁵ Certain satellite-based (Mobile Satellite System (MSS)) services, likewise, would fall in this category.

³⁶ Similarly included in this category would be other foreign-based or accessible customer service or call center services (regardless of carrier terminology employed for such and related endeavors) where there would be a database (or database access) containing, on an ongoing basis, comprehensive CPNI customer profile and/or billing information.

³⁷ As noted above, *inter alia*, espionage and economic espionage harms are interrelated with CPNI and, with foreign access, would be triggered concurrently with the range of other harms to privacy and confidentiality.

billing records of customers being available for multi-year periods of service.” As discussed above, by virtue of the CPNI being stored or accessible in a given foreign country, the laws of that country arguably could apply, conflicting with U.S. law and rendering such information open to selective *or* broad-scale undetectable and non-reportable foreign acquisition.

If it were the case that all telecommunications carriers offering service in the United States chose to store all CPNI abroad, it would immediately imperil vital U.S. law enforcement and national security investigations. As we explained in the *ex parte* letter at some length, it is absolutely imperative that U.S. law enforcement and national security agencies have unimpeded access to CPNI and other carrier subscriber records and information, pursuant to appropriate U.S. legal process.³⁹ Moreover, from the CPNI privacy and confidentiality perspective, even if maintaining a *copy* of the CPNI for all U.S. customers were to be mandated to meet vital U.S. law enforcement and national security *investigative* requirements, and even if carriers were to assure the U.S. government of access to such CPNI,⁴⁰ the foreign storage of customers’ original CPNI would nevertheless make possible all of the harms related to privacy and confidentiality abuse, economic and international espionage, and espionage-related “recruitment.”

In a number of the foreign ownership agreements that the DOJ and FBI have consummated, foreign storage of CPNI has not been precluded outright, so long as U.S. law enforcement or

³⁸ On the other hand, we do not find objectionable limited foreign access to such billing, marketing, call center, or other information systems for system development, maintenance, or similar support purposes, which may require (presumably brief) *incidental access* to U.S. Domestic Customer CPNI. *See* Comments of Ameritech at 1-2 (filed Mar. 30, 1998) with respect to limited “incidental access” to databases and systems. Hence, our views here are consistent with those above regarding very limited foreign access to CPNI with regard to international calling, roaming, MSS service, and switch and network development, maintenance, and trouble-shooting.

³⁹ *See* FBI *ex parte* letter at 4-8.

⁴⁰ *See, e.g.*, MCI Reply Comments at 19 (filed 4/14/98): “...MCI went the farthest in attempting to reach a compromise with the FBI on the issue by proposing that all domestic CPNI be readily accessible from the United States so that it is immediately available to law enforcement personnel.”).

intelligence agency have access to CPNI and stored communications, records, and other information upon service of appropriate legal process. We have taken this position in our agreements for several reasons. First, absent a rule of U.S. law with general application, we have been reluctant to insist upon *exclusive* U.S. storage in all cases. This docket offers the opportunity *to* remedy this matter on a comprehensive, as opposed to a selective, basis, with a rule applicable to all telecommunications carriers offering service in the United States. Second, in many *of* these agreements, the carrier was either principally offering international service or was conducting substantial business service internationally, as opposed to purely domestically. Third, each such agreement resulted from a careful *ad hoc* assessment of the likely potential for foreign storage of communications, records, and information (including CPNI) to actually occur” and, importantly, from a careful assessment with respect to the carrier and foreign country involved. Such *ad hoc* assessments, of course, are quite different from the matter before the Commission in this docket where, by virtue of the ruling of the Commission, a “green light” could potentially be given to *all* carriers offering service in the United States (domestic and foreign-based alike) to store the CPNI of U.S. Domestic Customers abroad. Fourth, although we have been prepared in our past agreements to tolerate foreign storage in particular cases, we can state unequivocally that there would be certain carriers and foreign countries which, if encountered in the context of Section 310(d) or Section 214 licensing applications, we would either oppose outright or obligate in an agreement to maintain CPNI and other stored data exclusively within the United States. Finally, in these agreements, there have also been provisions which require carriers to expressly advise the DOJ and the FBI of any potential plans

⁴¹ From our discussions and negotiations with the carriers in **these** agreements, it **has** been **our** understanding that the actual likelihood of foreign storage, although permitted in the agreement, was **typically** either **remote** or likely to be relatively limited in nature, scope, or duration.

to move stored subscriber communications, records and information (including CPNI) abroad, with the potential for further DOJ and FBI response.

With respect to the matter of foreign storage of CPNI or other stored communications, records and information, as discussed further below, certain carriers have commented that, even if the CPNI of U.S. customers were to be stored abroad, in their estimation there would be no real threat to U. S. law enforcement and national security agency efforts. They indicate that carriers could efficaciously honor U.S. legal process, just as they would be able to honor the dictates of CPNI protection. For several reasons such comments are both too facile in their assertion and unsound in their substance.

First, in the instant docket, no carrier offering its comments has acknowledged the implications of U.S. law (including the U.S. statutory and FCC regulatory laws with respect to CPNI) not applying exclusively to CPNI stored abroad – with all the attendant risks were foreign law to apply. Second, no carrier has considered the privacy and confidentiality implications of foreign-stored U.S. subscriber CPNI with respect to the undetectable and unreported access that foreign governmental entities (and perhaps others) could have to such CPNI (either “as required by law”⁴² or otherwise), by virtue of CPNI storage in a foreign country.⁴³ Third, no carrier has commented upon the implications of foreign law impediments to vital U.S. law enforcement and national security access to such foreign-stored CPNI – such as, for example, European laws requiring the destruction of CPNI immediately after it has served its technical or billing

⁴² Again, *see* discussion at 5, *supra*.

⁴³ Note, in this connection, the Comments of the Cellular Telecommunications Industry Association (CTIA) (dated Oct. 21, 2002) at 5: “. . . [international] GSM [Global System for Mobile Communications] Roaming Agreements ensure by contract that the customer’s information will be protected according to the domestic law of the place where the user is roaming” (emphasis added)

functions.⁴⁴ Fourth, no carrier, in offering its comments, has recognized the implications of existing or future⁴⁵ foreign legal impediments being asserted generally to U.S. agency access to foreign-stored CPNI material, and circumstances where the foreign government, in asserting its jurisdiction over the CPNI *res* in *its* land, may choose to oppose U.S. access (as we in fact would do (in the reverse) *to ensure compliance with U.S. law*, as indicated in our agreements). Fifth, some commenters, such as CTIA,⁴⁶ have cited the *Bank of Nova Scotia* ("BNS")⁴⁷ case, and the DOJ's United States Attorneys' Manual,⁴⁸ for the proposition that, even with foreign storage, there would be *no* impediment to U.S. agency access. This is incorrect. The BNS case simply upheld use of a subpoena to compel a U.S. branch of a bank to produce records held by a foreign branch of the same bank, even where production would violate the foreign country's bank secrecy laws. However, whether a court will enforce such a subpoena may depend on a balancing *of* factors relating to the facts of the specific case and the competing interests of the different sovereigns, so success is not a certainty⁴⁹. Moreover, use of such "BNS" subpoenas

⁴⁴ Compare Article 6 of Directive 2002/58/EC on Privacy and Electronic Communications, 2002 O.J. (L 201) 37, 44 ("Traffic data ... must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication ...") with 47 C.F.R. § 42.6 (1996) (common carriers are required to retain telephone toll records, a subset of CPNI, for a period of 18 months).

⁴⁵ We mention possible future foreign legal impediments because, internationally, the field of data destruction, preservation, and retention has been in tumultuous development in recent years.

⁴⁶ See CTIA's 2002 Comments (n. 16, *supra*) at 7.

⁴⁷ See *In Re Grand Jury Proceedings (Bank of Nova Scotia)* ("BNS"), 740 F.2d 817 (11th Cir.), *cert denied*, 469 U.S. 1106 (1985). In the BNS case, the records sought were bank records which rarely are time sensitive in nature. More importantly, the case stands for the proposition that a U.S. court will enforce U.S. law in the United States, notwithstanding that a foreign law may conflict with such U.S. law. The case does not speak to the reverse situation, where a foreign based entity might pursue its remedies in a foreign court which most likely would focus upon the foreign law and foreign interests.

⁴⁸ United States Attorney's Manual, Title 9, Criminal Division, available at http://www.usdoj.gov/usao/eousa/foia_reading_room/usam/index.html.

⁴⁹ *In Re Sealed Case*, 525 F.2d 494 (D.C. Cir. 1987).

may adversely affect the United States' law enforcement relationship with the foreign countries involved, and for this reason they are in fact used relatively infrequently and federal prosecutors must obtain written approval from the Criminal Division of the Department of Justice before issuing such subpoenas.”⁵⁰ Sixth, even if the carrier involved simply ignored the foreign law and caused the CPNI material to be accessed on behalf of the United States, it is entirely possible that the specific carrier access methodology or record-keeping regime may leave an electronic or other “audit trail” that could tip off the target, including a foreign-based national security target, and thus compromise an important investigation.”

Section III. Reply Comments

In this section, we address Comments made in this docket to date.

At the outset, some commenters question whether the matter raised by the FBI, with respect to recommended constraints being placed upon the foreign storage of and access to CPNI, should properly be before the Commission in this docket. Comments are made that the CPNI statute (47 U.S.C. § 222) is silent on the matter of storage of CPNI, and thus Section 222

⁵⁰ United States Attorney's Manual, Section 9-13.525. Alternatives to the “BNS” subpoena – seeking the assistance of a foreign country in obtaining the records through letters rogatory or Mutual Legal Assistance Treaties – are not uniformly successful, and even when successful they are far more burdensome on U.S. law enforcement authorities and entail significantly greater delay than the use of domestic legal process to obtain records located within the United States. Such alternatives also require disclosure to foreign authorities of the subject matter of the U.S. inquiry and the relevance of the records to that inquiry, disclosure which may not be appropriate in a particular case. Furthermore, the alternative of a letter rogatory or Mutual Legal Assistance Treaty request is available, if at all, only in the context of criminal investigations and prosecutions; it is not available in the national security context.

⁵¹ Omnipoint Communications, Inc. (Omnipoint) in its Comments at 8 (filed Mar. 31, 1998) suggested the use of security measures such as encryption to prevent foreign access. While the use of encryption can usefully be employed, as a purely technical matter, to protect the content of communications and otherwise, its value in protecting CPNI in a foreign billing center operation would probably not be practical nor effective. Assuming the CPNI was encrypted overseas, a foreign power could compel the possessor of the encrypted material to provide the keys (likely under the power of law). See, as a likely counterpart, CALEA § 103(b)(3) (requiring carriers to decrypt communications when they possess the information necessary to decrypt the communications). 47 U.S.C. § 1002 (b) (3). If the encryption were employed from the United States, the foreign power could still seize the encrypted material and seek to decrypt it on its own. Hence, encryption simply cannot solve the CPNI *exposure* problem.

cannot be a basis to regulate or control foreign storage or access;⁵² that, by virtue of Section 222's silence on these matters, Congress did not intend to regulate or control foreign storage or access;" and that such matters are accordingly outside the purview and power of the Commission to regulate.⁵⁴ We respectfully disagree.

The heart and spirit of Congress' CPNI statutory enactment is the protection of the privacy and confidentiality of U.S. customers' telecommunications records and information. We believe that the efforts required to effectuate the intended CPNI protection should be commensurate with the highly-sensitive nature of such CPNI records and information. As the Commission has noted, CPNI "consists of highly personal information."⁵⁵ Congress' enactment logically must be construed and implemented by the regulatory body charged with its proper effectuation in such a way that the law's central purpose will not be undermined and its central promise not broken, which must include making *essential* rulings related to foreign storage and access. When Congress enacted the CPNI law, there is every reason to believe that its intent was to secure, without further equivocation or exception, the privacy and confidentiality of U.S. telecommunications customers with respect to highly-personal CPNI information. With domestic storage of, and narrowly limited foreign access to, U.S.-based CPNI, Congress' will,

⁵² See, e.g., Comments of Iridium North America (INA) at 2-3 (filed Mar. 30, 1998); Reply Comments of INA at 1-2, 4 (filed April 14, 1998); Comments of Onmipoint at 7 (filed Mar. 31, 1998); Reply Comments of AT&T at 8 (filed April 14, 1998); Reply Comments of MCI Telecommunications Corporation (MCI) at 19, 22 (filed April 14, 1998); Comments of WorldCom, Inc. (WorldCom) at 8 (filed October 18, 2002); Reply Comments of US West, Inc. (US West) at 11 (filed April 14, 1998); Comments of CTIA at 2-3 (filed Oct. 21, 2002) Comments of Verizon at 2 (filed October 22, 2002).

⁵³ See, e.g., Comments of INA at 2-4 (filed Mar. 30, 1998); Reply Comments of INA at 4-5 (filed April 14, 1998); Reply Comments of US West at 11 (filed April 14, 1998); Reply Comments of MCI at 19 (filed April 14, 1998)

⁵⁴ See, e.g., Comments of WorldCom, Inc. (WorldCom) at 2, 8 (filed October 18, 2002); Comments of Verizon at 1-1 (filed October 22, 2002).

⁵⁵ See the Commission's *CPNI Order* at 48-49, ¶61; 13 FCC Rcd at 8108, ¶61

and the protection of CPNI if so desired, can be manifestly secured without any such equivocation or significant exception. However, as we have pointed out in this filing (as well as in the FBI *ex parte* letter), permitting sustained, ongoing, and broad-scale foreign storage of, or access to, U.S. Domestic Customers' CPNI could, by virtue of the operation and preemption of foreign law, substantially and undetectably eviscerate the privacy and confidentiality protections intended by Congress.

Like other statutory regimes whose promises are to be effectuated through subsequent regulation, there is no requirement for the CPNI statute to detail with complete specificity the manner and means of its implementation. Thus, the Commission, vested with broad and elastic powers⁵⁶ under the Communications Act, is authorized to effectuate the Congress' core intent and, through rulemaking, to issue rules with respect to the manner and means of implementing the privacy and confidentiality protections promised for CPNI.

The Commission's fundamental authority to rule here and to prescribe constraints upon the foreign storage of and access to U.S.-based CPNI is beyond dispute because such a ruling obviously, rationally, and directly gives meaningful effect both to the CPNI law and to the underlying privacy and confidentiality provisions which are at the core of the CPNI law. In the slightly different context of Commission jurisdiction to prescribe conditions under which terminal equipment may be interconnected with telephone networks, the Court of Appeals for the Fourth Circuit described the fullness of Commission regulatory authority: "The contention that the absence of explicit statutory authorization prevents the FCC from adopting a registration

⁵⁶ See *General Telephone Co. of Southwest v. United States*, 449 F.2d 846, 853 (5th Cir. 1971) ("The Communications Act **was** designed to endow the Commission with sufficiently elastic powers such that it could readily accommodate dynamic new developments in the field of communications.")

program [for terminal equipment] contradicts all relevant authority⁵⁷ and confounds the very purpose of agency delegation -- institutionalization of authority *to* fashion policies and programs that implement broad legislative mandates in presently unforeseeable circumstances.”⁵⁸

Similarly, the United States Supreme Court has stated, “In the context of the developing problems to which it was directed, the [Communications] Act gave the Commission not niggardly but expansive powers.”” Elsewhere the United States Supreme Court has stated, “Nothing in the language of §152(a) [of the Communications Act of 1934], in the surrounding language, or in the Act’s history or purposes limits the Commission’s authority *to those activities* and forms of communication that are specifically described by the Act’s other provisions.” (emphasis added)“

Further, as noted in Section I, *supra*, the first stimulus with respect to referring this matter to the Commission was the *agreed-to understanding* of the telecommunications carriers BT, MCI, and Concert, plc, and the FBI and DOD, that the current CPNI docket was both Jurisdictionally empowered and entirely appropriate to rule on this matter of foreign storage of and access to domestic CPNI. Moreover, both in its consultation with the aforementioned parties during negotiation of the BT-MCI agreement, and subsequently, when the Commission reviewed, approved, and ultimately adopted the agreement with all of its provisions, there was

⁵⁷ Footnote in the original quoted text: “E.g., *National Broadcasting Co. v. United States*, 319 U.S. 190, 218-19 (1943) (FCC power to take action not explicitly authorized by Communications Act upheld; “itemized catalogue” of specific problems and powers of a regulatory agency would “frustrate the purposes for which the Communications Act” was passed); *GTE Service Corp. v. FCC*, 474 F.2d 724, 730-31 (2d Cir. 1973) (fact that Communications Act makes no reference to computers and data processing does not prohibit FCC from regulating carrier activities in those fields); *Mt. Mansfield Television, Inc. v. FCC*, 442 F.2d 470, 480-81 (2d Cir. 1971) (FCC may regulate prime time access in television despite lack of specific statutory authorization).”

⁵⁸ *North Carolina Utilities Commission v. F.C.C.*, 552 F.2d 1036, 1051 (4th Cir.), *cert. denied*, 434 U.S. 874 (1977).

⁵⁹ *National Broadcasting Co. v. United States*, 319 U.S. 190, 219 (1943).

⁶⁰ *United States v. Southwestern Cable Co.*, 392 U.S. 157, 172 (1968).

never any hint or suggestion from the Commission that this matter was not subject to regulation and proscription under Section 222 of the Communications Act and the Commission's implementing rules. Nor was there any indication that the Commission otherwise lacked jurisdiction or authority to treat this CPNI matter. The Commission was correct in its jurisdictional assessment then, and the Commission should reassert it now, recognizing that "[t]he FCC's interpretation and application of its authorizing statute... will be set aside only if it is 'arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law.' 5 U.S.C. § 706(2)(A) (1982)."⁶¹

A number of commenters also have taken the position that the CPNI rules enunciated in Section 222 adequately protect customers' privacy and confidentiality rights.⁶² We respectfully disagree with this contention. First of all, as amply discussed throughout this Comment and in the prior *ex parte* letter, the operation of foreign law in the foreign country in which the CPNI might be stored or accessed may as a practical matter conflict with Section 222. Further, as pointed out, foreign law and foreign governmental actions contrary to the privacy and confidentiality provisions of Section 222 can be undertaken without detection or reporting. Moreover, as a practical and legal matter, there is no effective way for the domestic carrier, the Commission, or other United States Government agencies to inspect or investigate the uses and disclosures of foreign-located CPNI.

Several commenters have stated that the FBI recommendation would conflict with

⁶¹ *Rural Telephone Coalition v. F.C.C.*, 838 F.2d 1307, 1313 (D.C. Cir. 1988) (construing the Commission's ability to interpret and apply its jurisdiction and authority consistent with the dictates of the Administrative Procedures Act.)

⁶² See, e.g., INA Comments at 2, 4 (filed Mar. 30, 1998); INA Reply Comments at 2 (filed April 14, 1998); MCI Comments at 19 (filed Mar. 30, 1998); GTE Comments at 7-8 (filed Mar. 30, 1998)

international calling and roaming.⁶³ As we have explained in Section II above, the recommendation proposed clearly would *not* constrain international calling or roaming because the foreign storage and access involved in such circumstance would be very limited in its nature, scope and duration. That is, CPNI transmitted, temporarily stored, and briefly accessible abroad pursuant to the placement of international calls and roaming would *not* be subject to the rule proposed. Similarly, several commenters have indicated that, in their view, the FBI recommendation would conflict with *foreign-based* switch, gateway, or network support.⁶⁴ Again, as we explained in Section II above, the recommendation proposed clearly would *not* constrain foreign-based switch, gateway, or network support because the foreign storage and access involved would be very limited in its nature, scope and duration. Likewise, CPNI temporarily stored and accessible abroad pursuant to the development, maintenance, and troubleshooting required to support switches, gateways, and communications networks would *not* be subject to the rule proposed. On the other hand, the recommended action for Commission rulemaking should be applied to the sustained, ongoing and broad-scale storage of and access to such CPNI by and through foreign-based billing, marketing, call center, and similar entities where the foreign storage and access to Domestic Customer CPNI are *not* limited in nature, scope, and duration.

Commenters have also indicated that there may be cost savings in having the CPNI of U.S. Domestic Customers stored abroad or accessible from abroad, and that a constraint on

⁶³ See, e.g., Comments of AT&T Wireless, Inc. (AWS) at 2-4, 8 (filed Oct. 21, 2002); Omnipoint Comments at 8 (filed Mar. 30, 1998). Omnipoint Reply Comments at 5-6 (filed April 14, 1998); Nextel Communications, Inc. (Nextel) at 4, filed Oct. 21, 2002; INA Comments at 5-9 (filed Mar. 30, 1998); INA Reply Comments at 2-3 (filed April 14, 1998).

⁶⁴ See, e.g., INA Comments at 6-9 [filed Mar. 30, 1998]; Ameritech Comments at 2 (filed Mar. 30, 1998); CTIA Comments at 4-5 (filed Oct. 21, 2002).

foreign storage or access to domestic CPNI could cause carriers to incur greater expense.⁶⁵ The foregoing proposition is irrelevant to the fundamental thrust of Section 222 and the privacy and confidentiality protections it promises. As we have explained above, placing the CPNI of Domestic Customers abroad, such that there is sustained, ongoing, and broad-scale foreign access to the CPNI, clearly imperils the privacy and confidentiality of such CPNI in ways that Section 222 simply cannot prevent (by virtue of the application of foreign law in the foreign land).

It has only been within the last few years that carriers have been considering or actually storing or accessing domestic CPNI abroad. Before then it had been the traditional, pervasive, and completely commonplace circumstance that such CPNI was virtually *always* stored exclusively within or accessed exclusively from within the United States. We are unaware of any significant affirmative carrier complaint arising during this period of **exclusive** U.S. domestic storage of CPNI that such domestic storage was burdensome or onerous. Thus, carriers cannot now plausibly claim that returning to the former (and recent) status quo would be intolerable. Neither can they, by invoking the mantra of globalization, cause the privacy and confidentiality of Americans' CPNI to be depreciated when palpable foreign-based risks have been identified. While carriers may logically seek to reduce expenses in all areas of corporate endeavor, the Commission cannot partner with carriers in this regard when the privacy and confidentiality of Americans' CPNI (which the Commission is tasked with preserving in this docket) are at risk. Further, neither can the Commission endorse carriers' recent appetite for thriftiness with respect to the foreign storage of CPNI when vital U.S. law enforcement and national security interests

⁶⁵ See, e.g., Comments of MCI at IS-19 (filed Mar. 30, 1998); Comments of Nextel at 5-6 (filed Oct. 21, 2002); CTIA Comments at 4 (filed Oct. 21, 2002); AT&T Reply Comments at 8-9 (filed April 14, 1998); Comments of Verizon at 3-4 (filed October 22, 2002).

(requiring sure, secure, expeditious, and unimpeded U.S. investigative access to CPNI) would be jeopardized.

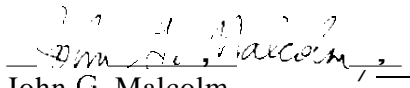
Conclusion:

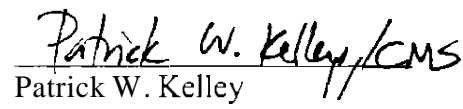
In conclusion, as explained above, we believe the Commission is fully empowered to make essentially-needed rules with respect to the foreign storage of and access to the CPNI of U.S. customers under its implementation of Section 222. Only by constraining foreign storage and access to such CPNI records can the statute reflecting Congress' intent be effectively carried out. As noted above, with the foreign storage of, or broad scale foreign access to, CPNI, U.S. law (with respect to 47 U.S.C. § 222, 18 U.S.C. § 2703, and others) cannot be said to be exclusively controlling. This circumstance opens the door to litigation over the possible conflict of foreign law with U.S. law and its privacy and confidentiality protections in this area. Indeed, the language of Section 222 ("except as required by law") may be cited by foreign governments (acting pursuant to foreign legal process or otherwise) as justification to access and use U.S. customer CPNI in ways that are completely contrary to U.S. privacy, business-proprietary, law enforcement, national security, international espionage, and economic espionage interests. Moreover, as pointed out, such access and use could occur narrowly or quite broadly, and completely transparently without any detection by or reporting to the United States.

In this filing we have made clear that we do not propose to constrain foreign access to or storage of the CPNI of U.S. Domestic Customers when such access or storage is brief and *limited in its nature, scope, and duration*. However, the Commission would be countenancing the array of harms identified in this Comment if it were to permit the sustained, ongoing, and broad-scale foreign storage of and access to CPNI through foreign-based billing, marketing, and

call center facilities which so obviously and readily lend themselves to foreign governmental access. The Commission should not stand by and permit the privacy and confidentiality of Americans' CPNT, nor the inextricably linked U.S. law enforcement and national security interests, to be placed at risk

Respectfully submitted.


John G. Malcolm
Deputy Assistant Attorney General
Criminal Division
UNITED STATES DEPARTMENT OF
JUSTICE
10th Street & Constitution Avenue, N.W.
Washington, D.C. 20530
(202) 616-3928


Patrick W. Kelley
Deputy General Counsel
FEDERAL BUREAU OF INVESTIGATION
935 Pennsylvania Avenue, N.W.
Washington, D.C. 20535
(202) 324-6829

November 19, 2002

CERTIFICATE OF SERVICE

I, Myla R. Saldivar-Trotter, Federal Bureau of Investigation, hereby certify that on this 19th day of November, 2002, I caused a true and correct copy of the foregoing **Reply Comments of the U.S. Department of Justice and the Federal Bureau of Investigation** to be served via hand delivery (indicated by *) or by mail to the following parties:

William Maher*
Bureau Chief, Office of the Bureau Chief
Wireline Competition Bureau
Federal Communications Commission
445 12th St. SW
Washington, D.C. 20554

James D. Schlichting*
Deputy Chief
Wireless Telecommunications Bureau
Federal Communications Commission
445 12th St., SW
Washington, D.C. 20554

Marcy Greene*
Attorney Advisor, Competition Policy Division
Wireline Competition Bureau
Federal Communications Commission
445 12th St., SW
Washington, D.C. 20554

Howard J. Symons
Sara F. Leibman
Susan S. Ferrel
Mintz, Levin, ~~Colin~~ Ferris, Glovsky and Popeo, P.C.
701 Pennsylvania Avenue, NW
Suite 900
Washington, D.C. 20004
Of Counsel for AT&T Wireless Services, Inc.

Ann H. Rakeshaw
Attorney for Verizon Telephone Companies
Edward Shakin
Michael E. Glover
Of Counsel for Verizon Telephone Companies
Suite 500
1515 North Courthouse Road
Arlington, VA 22201

Thomas J. Sugrue*
Chief
Wireless Telecommunications Bureau
Federal Communications Commission
445 12th St., SW
Washington, D.C. 20554

Jeffrey Carlisle*
Sr. Deputy Chief, Office of the Bureau Chief
Wireline Competition Bureau
Federal Communications Commission
445 12th St. SW
Washington, D.C. 20554

Sharon J. Devine
Kathryn Marie Krause
Suite 700
1020 19th Street, NW
Washington, D.C. 20036
Counsel for Qwest Services Corporation

Douglas I. Brandon,
Vice President - External Affairs
David P. Wye
Director - Spectrum Policy
1150 Connecticut Avenue, NW
Suite 400
Washington, D.C. 20036

Lawrence E. Sarjeant
Indra Sehdev Chalk
Michael T. McMenamin
Robin E. Tuttle
1401 H Street, NW
Suite 600
Washington, D.C. 20005
Counsel to United States Telecom Association

Leonard J. Kennedy
Sr. Vice President & General Counsel
Celeste M. Moy
Vice President & Associate General Counsel
Nexitel Communications, Inc.
2001 Edmund Halley Drive
Reston, VA 20191

Michael Altschul
Sr. Vice President & General Counsel
Cellular Telecommunications & Internet
Association
1250 Connecticut Avenue, NW
Suite 800
Washington, D.C. 20036

Robert M. Lynch
Durard D. Dupre
Michael J. Zpevak
Robert J. Gryznala
One Bell Center
Room 3532
St. Louis, MO 63101
Counsel for SBC Communications, Inc. and
its subsidiaries

Daniel Meron
Jonathan F. Colm
Sidley Austin Brown & Wood LLP
1501 K Street, NW
Washington, D.C. 20005
Counsel for AT&T Corp.
Michael B. Fingerhut
Richard Juhnke
401 9th Street, NW
Suite 400
Washington, D.C. 20004
Counsel for Sprint Corp.
Michael S. Fabian
Room 4H82
2000 West Ameritech Center Drive
Hoffman Estates, IL 60196-1025
Counsel for Ameritech

To-Quyen T. Truong
Christina H. Burrow
Dow, Lohnes & Albertson, PLLC
1200 New Hampshire Avenue, N.W.
Washington, D.C. 20036
Counsel for Nextel Communications, Inc.

Davida Grant
Gary L. Phillips
Paul K. Mancini
SBC Communications, Inc.
1401 I Street, NW
4th Floor
Washington, D.C. 20005
Counsel for SBC Communications, Inc.

Karen Reidy
1133 19th Street, NW
Washington, D.C. 20036
Counsel for WORLDCOM, Inc.

Mark C. Rosenblum
Lawrence J. Lafaro
Judy Sello
AT&T Corp., Room 3A229
900 Route 202/206 North
Bedminster, NJ 07921

Jonathan E. Canis
Kelly Drye & Warren LLP
1200 Nineteenth Street, NW
Suite 500
Washington, D.C. 20036
Counsel for Intermdia Communications, Inc.

Frank W. Krogh
Mary L. Brown
1801 Pennsylvania Avenue, NW
Washington, D.C. 20006
Counsel for MCI Telecommunications Corporation

Philip L. Malet
James M. Talens
Tekedra V. McGee
Stoptoc & Johnson LLP
1330 Connecticut Avenue, NW
Washington, D.C. 20036
Counsel for Iridium North America

Gail L. Polivy
GTE Service Corporation
1850 M Street, NW
Washington, D.C. 20036

Stephen L. Earnest
Richard M. Sbaratta
Suite 4300
675 West Peachtree Street, NE
Atlanta, CA 30375
Counsel for BellSouth Corporation

Marc Rotenberg
Mikal Condon
Electronic Privacy Information Center
1718 Connecticut Avenue, NW
Suite 200
Washington, D.C. 20008

Peter Anh. Jr.
Edward W. O'Neill
Mary Mack Adu
Attorneys for the People of the State of California
and the Public Utilities Commission of the
State of California
505 Van Ness Avenue
San Francisco, CA 94102

Michael G. Hoffman
Patricia Zacharie
1600 Viceroy Dr.
Dallas, TX 75235
Counsel for VarTeeD Telecom. Inc.

John E. Logan
1050 Connecticut Avenue, NW
Tenth Floor
Washington, D.C. 20036
Counsel for ATX Technologies

John F. Raposa
Richard McKenna
GTE Service Corporation
600 Hidden Ridge, HQE03J36
P O Box 152092
Irving, TX 75015-2092

Charon J. Harris
Stephen J. Berman
Verizon Wireless
1300 I Street, NW
Suite 400-W
Washington, D.C. 20005

James Bradford Ramsey
1101 Vermont Avenue, NW
Suite 200
Washington, D.C. 20005
Counsel for NARUC

David Cosson
L. Marie Guillory
NTCA
2626 Pennsylvania Avenue, NW
Washington, D.C. 20037

Cynthia B. Miller, Esquire
Bureau of Intergovernmental Liaison
Florida Public Service Commission
2540 Shumard Oak Boulevard
Tallahassee, FL 32399-0872

Glenn S. Rabiii
ALLTEL Corporation
601 Pennsylvania Avenue
Suite 720
Washington, DC 20004

Charles C. Hunter
Catherine M. Hannan
Hunter Communications Law Group
1424 Sixteenth Street, NW
Suite 105
Washington, D.C. 20036
Counsel for ASCENT

Lisa M. Zaina
Stuart Polikoff
OPASTCO
21 Dupont Circle NW
Suite 700
Washington, D C 20036

Kareti Brinkman
Tonya Rutherford
Latham & Watkins
suite 1000
555 Eleventh Street. NW
Washington, D.C. 20004-1304
Counsel for CenturyTel, Inc.

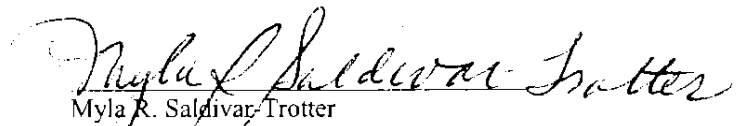
Ian D. Volner
Rita L. Brickman
Venable, Baetjer, Howard & Civiletti, LLP
1201 New York Avenue, NW
Washington , D.C. 20005-3917
Counsel for Direct Marketing Association

Russell J. Zuckerman
Francis D. R. Coleman
175 Sully's Trail
Suite 300
Pittsford, NY 14534
Counsel for Mpower Communications

Ronald J. Binz
Debra Berlyn
John Windhausen
Competition Policy Institute
1156 15th Street, NW
Suite 310
Washington, D.C. 20005

J.R. Carbonell
Carol L. Tacker
David G. Richards
5565 Glenridge Connector, Suite 1700
Atlanta, GA 30342
Counsel for Cingular Wireless, LLC

Albert Gidari
Perkins Coie, LLP
505 Fifth Avenue South
Suite 620
Seattle, WA 98104
Counsel for Intellione, Inc


Myla R. Saldivar-Trotter